This document is scheduled to be published in the Federal Register on 04/24/2013 and available online at **http://federalregister.gov/a/2013-09619**, and on **FDsys.gov**

DEPARTMENT OF DEFENSE **Billing Code 5001-06**

Office of the Secretary

32 CFR Part 329

[Docket ID: DOD-2012-OS-0161]

RIN 0790-AI96

National Guard Bureau Privacy Program

AGENCY: Department of Defense.

ACTION: Proposed rule.

SUMMARY: This proposed rule establishes policies and procedures for the National Guard Bureau (NGB) Privacy Program. The NGB is a Joint Activity of the Department of Defense (DoD). This rule will cover the privacy policies and procedures associated with records created and under the control of the Chief, NGB that are not otherwise covered by existing DoD, Air Force, or Army rules.

DATES: Comments must be received by [insert 60 days from date of publication]

ADDRESSES: You may submit comments, identified by docket number and or RIN number and title, by any of the following methods:

- Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Mail: Federal Docket Management System Office, 4800 Mark Center Drive, East Tower, Suite 02G09, Alexandria, VA 22350-3100.

Instructions: All submissions received must include the agency name and docket number or Regulatory Information Number (RIN) for this FR document. The general policy for comments and other submissions from members of the public is to make these

submissions available for public viewing on the Internet at http://regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Jennifer Nikolaisen, 571-256-7838

SUPPLEMENTARY INFORMATION:

EXECUTIVE SUMMARY

I. Purpose and Authority of the Regulatory Action

a. Purpose: This part implements the policies and procedures outlined in 5 U.S.C. 552a, Office of Management and Budget (OMB) Circular No. A-130, and 32 CFR part 310. This part provides guidance and procedures for implementing the National Guard Bureau Privacy Program. The NGB is a Joint Activity of the DoD pursuant to 10 U.S.C. 10501

b. Authority: Pub. L. 93–579, 88 Stat. 1986 (5 U.S.C. 552a).

II. Summary of the Major Provisions of the Regulatory Action

This provision is made to establish the Privacy Program for the National Guard Bureau.

III. This regulatory action imposes no monetary costs to the Agency or public. The benefit to the public is the accurate reflection of the Agency's Privacy Program to ensure that policies and procedures are known to the public.

REGULATORY PROCEDURES

Executive Order 12866, "Regulatory Planning and Review" and Executive Order 13563, "Improving Regulation and Regulatory Review"

It has been determined that 32 CFR part 329 is not a significant regulatory action. The rule does not:

(1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy; a section of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities;

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency;

(3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or

(4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in these Executive Orders.

Unfunded Mandates Reform Act (Sec. 202, Public Law 104-4)

It has been certified that this rule does not contain a Federal mandate that may result in the expenditure by State, local and tribal governments, in aggregate, or by the private sector, of $100 million or more in any one year.

Public Law 96-354, "Regulatory Flexibility Act" (5 U.S.C. 601)

It has been certified that this rule is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities.

Public Law 96-511, "Paperwork Reduction Act" (44 U.S.C. Chapter 35)

It has been certified that this rule does not impose reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995.

Executive Order 13132, "Federalism"

It has been certified that this rule does not have federalism implications, as set forth in Executive Order 13132. This rule does not have substantial direct effects on:

(1) The States;

(2) The relationship between the National Government and the States; or

(3) The distribution of power and responsibilities among the various levels of Government.

List of Subjects in 32 CFR Part 329

Privacy

Accordingly, 32 CFR part 329 is proposed to be added to read as follows:

PART 329- NATIONAL GUARD BUREAU PRIVACY PROGRAM

Sec.

Authority: Pub. L. 93–579, 88 Stat. 1986 (5 U.S.C. 552a).

§ 329.1 Purpose.

This part implements the policies and procedures outlined in 5 U.S.C. 552a, Office of Management and Budget (OMB) Circular No. A-130, and 32 CFR part 310. This part

provides the responsibilities, guidance, and procedures for the National Guard Bureau (NGB) to comply with Federal and DoD Privacy requirements.

§ 329.2 Applicability.

(a) This part applies to the NGB and the records under the custody and control of the Chief, NGB, as defined by DoD Directive (DoDD) 5105.77, entitled "National Guard Bureau"(**Available at http://www.dtic.mil/whs/directives/corres/pdf/510577p.pdf**)

(b) It does not apply to the National Guards of the States, Territories, and District of Columbia, except to the extent that they are in the possession of NGB records or relying on a System of Records Notice (SORN) published by NGB for their authority to maintain 5 U.S.C. 552a protected records.

§ 329.3 Definitions.

All terms used in this part which are defined in 5 U.S.C. 552a shall have the same meaning herein.

Access. Allowing individuals to review or receive copies of their records.

Accuracy. Within sufficient tolerance for error to assure the quality of the record in terms of its use in making a determination.

Agency. Any Executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the [federal] Government (including the Executive Office of the President), or any independent regulatory agency (as defined by 5 U.S.C. 552a).

Amendment. The process of adding, deleting, or changing information in a System of Records (SOR) to make the data accurate, relevant, timely, and/or complete.

Appellate Authority. The individual with authority to deny requests for access or amendment of records under 5 U.S.C. 552a.

Breach. A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where a person other than authorized users (with an official need to know), and for an other than authorized purpose has access or potential access to personally identifiable information, whether physical or electronic. A breach can include identifiable information in any form. (As defined by DoD Director of Administration and Management Memo, 5 Jun 2009 entitled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)"(Available at http://www.dod.mil/pubs/foi/privacy/docs/DA_M6_5_2009Responding_toBreach_of_PII).)

Chief, National Guard Bureau (CNGB). A principal advisor to the Secretary of Defense, through the Chairman of the Joint Chiefs of Staff, on matters involving non-federalized National Guard forces and on other matters as determined by the Secretary of Defense; and the principal adviser to the Secretary of the Army and the Chief of Staff of the Army, and to the Secretary of the Air Force and the Chief of Staff of the Air Force, on matters relating to the National Guard, the Army National Guard of the United States, and the Air National Guard of the United States. The CNGB also represents the National Guard on the Joint Chiefs of Staff.

Completeness. All elements necessary for making a determination are present before such determination is made.

Computer Matching Program. A program that matches the personal records in computerized database of two or more Federal agencies.

Denial Authority. The individual with authority to deny requests for access or amendment of records under 5 U.S.C. 552a.

Determination. Any decision affecting an individual which, in whole or in part, is based on information contained in the record and which is made by any person or agency.

Directorate/Division. The terms directorate and division are used to refer to suborganizations within the NGB. The Joint Staff and Air Guard Readiness Center uses the term "Directorate" to refer to their suborganizations and the Army Guard Readiness Center uses the term "Division" to refer to their suborganizations.

Disclosure. Giving information from a system, by any means, to anyone other than the record subject.

Disclosure Accounting. A record of all disclosures made from a SOR, except for disclosures made to Department of Defense personnel for use in performance of their official duties or disclosures made as required by 5 U.S.C. 552.

Federal Register (FR). A daily publication of notices and rules issued by Federal Agencies and the President printed on a daily Federal workday.

Individual. A citizen of the United States or an alien lawfully admitted for permanent residence. (As defined by 5 U.S.C. 552a)

Maintain. Maintain, collect, use or disseminate. (As defined by 5 U.S.C. 552a)

Memorandum of Agreement. A written understanding (agreement) between parties to cooperatively work together on an agreed upon project or meet an agreed objective.

Memorandum of Understanding. A written agreement between parties describing a bilateral or multilateral agreement between parties.

Necessary. A threshold of need for an element of information greater than mere relevance and utility.

Personal Information. Information about an individual other than items of public record.

Personally Identifiable Information (PII). Personal information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her. Information which can be used to distinguish or trace an individual's identity which is linked or linkable to a specified individual.

Privacy Act (5 U.S.C. 552a) Request. An oral (in person) or written request by an individual to access his or her records in a SOR.

Privacy Act (5 U.S.C. 552a) Statement (PAS). A statement given to an individual when soliciting personal information that will be maintained in a SOR that advises them of the authority to collect information, the principal purpose(s) that the information will be used for, the routine uses on how the information will be disclosed outside of the agency, and whether it is mandatory or voluntary to provide the information and any consequences for not providing the information.

Privacy Impact Assessment (PIA). A written assessment of an information system that addresses the information to be collected, the purpose and intended use; with whom the information will be shared; notice or opportunities for consent to individuals; how the information will be secured; and whether a new SOR is being created under 5 U.S.C. 552a. Privacy Impact Assessments are required for all information systems and electronic collections that collect, maintain, use, or disseminate personally identifiable

information about members of the public (this includes contractors and family members), under Public Law 107-347, Section 208 of the E-Government Act of 2002. DoD Instruction 5400.16, entitled "Department of Defense Privacy Impact Assessment (PIA)"(Available at http://www.dtic.mil/whs/directives/corres/pdf/540016p.pdf), provides additional requirements for PIAs, including a requirement to write a PIA on any information systems or electronic collection of PII on Federal personnel.

Protected Health Information (PHI). Any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

Record. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph (As defined by 5 U.S.C. 552a).

Relevance. Limitation to only those elements of information that clearly bear of the determination(s) for which the records are intended.

Routine Use. The disclosure of a record outside the DoD for a use that is compatible with the purpose for which the information was collected and maintained by the DoD. The routine use must be included in the published system notice for the SOR involved. The DoD Blanket Routine Uses, found in 32 CFR part 310, Appendix C are applicable to all SORNs published by DoD.

System Manager. The official who is responsible for managing a SOR, including policies and procedures to operate and safeguard it. Local System Managers operate record

systems or are responsible for the records that are maintained in decentralized locations but are covered by a SORN published by another DoD activity or a Government-Wide SORN.

System of Records (SOR). A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

System of Records Notice (SORN). The official public notice published in the FR of the existence and content of the SOR. As required by 5 U.S.C. 552a and 32 CFR part 310, Appendix E. The notice shall include:

(1) The name and location of the system,

(2) The categories of individuals on whom records are maintained in the system,

(3) The categories of records maintained in the system,

(4) Each routine use of the records contained in the system, including the categories of users and the purpose of such use,

(5) The policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records,

(6) The title and business address of the agency official who is responsible for the SOR,

(7) The agency procedures whereby an individual can be notified at his request if the SOR contains a record pertaining to him,

(8) The agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the SOR, and how he can contest its contents; and

(9) The categories of sources of records in the system

Timeliness. Sufficiently current to ensure that any determination based on the record will be accurate and fair.

§ 329.4 Policy.

In accordance with 32 CFR part 310, it is NGB's policy that:

(a) Personal information contained in any SOR maintained by any NGB organization will be safeguarded to the extent authorized by 5 U.S.C. 552a, Appendix I of Office of Management and Budget Circular No. A-130, and any other applicable legal requirements.

(b) NGB will collect, maintain, use, and disseminate personal information only when it is relevant and necessary to achieve a purpose required by a statute or Executive Order.

(c) NGB will collect personal information directly from the individuals to whom it pertains to the greatest extent possible and will provide individuals a PAS at the time of collection when the information being collected will be filed and/or retrieved by the subject's name or other unique identifier. The PAS will contain the following elements, as required by 5 U.S.C. 552a:

(1) The statutory authority or Executive Order that allows for the solicitation,

(2) The intended use/purpose that will be made of the information collected,

(3) The routine uses that may be made of the information collected; and

(4) Whether it is mandatory or voluntary for the individual to disclose the requested information and the non-punitive effects on the individual for not providing all or any part of the requested information. Collection can only be mandatory if the statutory authority or Executive Order cited provides a penalty for not providing the information.

(d) NGB offices maintaining records and information about individuals will ensure that such data is protected from unauthorized access, use, dissemination, disclosure, alteration, and/or destruction. Offices will establish safeguards to ensure the security of personal information is protected from threats or hazards that might result in substantial harm, embarrassment, inconvenience, or unfairness to the individual using guidelines found in 32 CFR part 310, subpart B, 32 CFR part 310, Appendix A, and DoD Manual (DoDM) 5200.01, Volume 4, entitled "DoD Information Security Program: Controlled Unclassified Information (CUI)"(Available at http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf)."

(e) NGB offices shall permit individuals to access and have a copy of all or any portion of records about them, unless an exemption for the system has been properly established (see 5 U.S.C. 552a, 32 CFR part 310, subparts D and F, and section 7 of 32 CFR part 329). Individuals requesting access to their record will also receive concurrent consideration under 5 U.S.C. 552 and 32 CFR part 286.

(f) NGB offices will permit individuals an opportunity to request that records about them be corrected or amended (see 5 U.S.C. 552a, 32 CFR part 310, subpart D, and part 6 of 32 CFR part 329).

(g) Any records about individuals that are maintained by the NGB will be maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual before making any determination about the individual or before making the record available to any recipient pursuant to a routine use.

(h) NGB will keep no record that describes how individuals exercise their rights guaranteed by the First Amendment, unless expressly authorized by statute or by the

individual to whom the records pertain, or is pertinent to and within the scope of an authorized law enforcement activity.

(i) NGB will notify individuals whenever records pertaining to them are made available under compulsory legal processes, if such process is a matter of public record.

(j) NGB will assist individuals in determining what records pertaining to them are being collected, maintained, used, or disseminated.

(k) NGB offices and personnel, including contractors, maintaining and having access to records and information about individuals will manage them and conduct themselves so as to avoid the civil liability and criminal penalties provided for under 5 U.S.C. 552a.

§ 329.5 Responsibilities.

(a) Chief of the National Guard Bureau (CNGB). The CNGB, under the authority, direction, and control of the Secretary of Defense (SecDef), approves and establishes overall policy, direction, and guidance for the NGB privacy program and promulgates privacy policy for the non-Federalized National Guard.

(b) NGB Chief Counsel. The NGB Chief Counsel, under the authority, direction, and control of the CNGB, shall:

(1) Serve as the National Guard Senior Component Official for Privacy (SCOP) pursuant to part 32 CFR part 310, subpart A.

(2) Direct and administer the Privacy Program for the NGB as well as the National Guard of the States, Territories, and the District of Columbia as it pertains to the maintenance of records protected by 5 U.S.C. 552a, other Federal laws on privacy, and OMB and DoD Privacy policies.

(3) Ensure implementation of and compliance with standards and procedures established by 5 U.S.C. 552a, OMB A-130, 32 CFR part 310, and this part.

(4) Serve as the appellate authority on denials of access or amendment.

(5) Direct the implementation all aspects of 5 U.S.C. 552a, OMB A-130, 32 CFR part 310, this part, and other Federal laws on privacy, and OMB and DoD Privacy policies.

(c) Chief of the Office of Information and Privacy (OIP). The Chief of the OIP, under the authority, direction, and control of the NGB Chief Counsel, shall:

(1) Oversee the National Guard's compliance with 5 U.S.C. 552a, OMB A-130, 32 CFR part 310, this part, and other Federal laws on privacy, and OMB and DoD Privacy policies.

(2) Issue policy and guidance as it relates to 5 U.S.C. 552a and other Federal and DoD Privacy requirements.

(3) Collect, consolidate, and submit Privacy reports to the Defense Privacy and Civil Liberties Office (DPCLO), or the respective service (Air Force or Army) that the reporting of information pertains to. This includes, but is not limited to:

(i) Personally Identifiable Information (PII) Breach Reports required by 32 CFR part 310, subpart B,

(ii) Quarterly Training Reports, SORN Reviews, Privacy Complaints, and Privacy Officer Activity Reports required by 32 CFR part 310, subpart I; and,

(iii) Reports pursuant to sec. D of 44 U.S.C. 3541 and Public Law 17-347.

(4) Submit all approved SORNs to the DPCLO or the respective service that has the statutory authority to publish the SORN for publication in the FR.

(5) Refer inquiries about access, amendments of records, and general and specific exemptions listed in a SORN to the appropriate System Manager.

(6) Review all instructions, directives, publications, policies, Memorandums of Agreement (MOA), Memorandums of Understanding (MOU), data sharing agreements, data transfer agreements, data use agreements, surveys (including web-based or electronic), and forms that involve or discuss the collection, retention, access, use, sharing, or maintenance of PII are to ensure compliance with this part.

(7) Make training resources available to NGB personnel, including contractors, regarding 5 U.S.C. 552a, OMB A-130, 32 CFR part 310, compliance with this part, and other Federal and DoD Privacy requirements.

(d) Chief of Administrative Law. The Chief of Administrative Law shall serve as the initial denial authority (IDA) to deny official requests for access or amendment to an individual's record pursuant to a published NGB SORN under 5 U.S.C. 552a or amendments to such records.

(e) Chief of Litigation and Employment Law. The Chief of Litigation and Employment Law will notify the Chief of the OIP of any complaint citing 5 U.S.C. 552a is filed in a U.S. District Court against the NGB, or any employee of NGB using the procedures outlined in section 6 of 32 U.S.C. part 329.

(f) NGB Comptroller/Director of Administration and Management (DA&M). The NGB Comptroller/DA&M shall ensure appropriate Federal Acquisition Regulation (FAR)(**Available at https://www.acquisition.gov/far/**) and Defense Federal Acquisition Regulation Supplement (DFARS)(**Available at http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html)** clauses (FAR

Subpart 24.1 related to 5 USC 552a and FAR subpart 24.2 related to 5 U.S.C. 552, as well as DFARS clauses 52.224-1 and/or 52.224-2) are included in all contracts that provide for contractor personnel to have access or maintain records, including records in information systems, that are covered by 5 U.S.C. 552a or that contain PII.

(g) NGB Directorates/Divisions. All NGB directorates/divisions maintaining records containing PII or that have personnel that have access to PII shall:

(1) Ensure that a SORN is published in the FR before collection of any information subject to 5 U.S.C. 552a is scheduled to begin.

(2) Ensure System Managers comply with all responsibilities outlined in section 5(h) of 32 U.S.C. part 329. This includes referring any proposed denials of access or amendment under 5 U.S.C. 552a to the Chief of the OIP within 10 working days.

(3) Evaluate Privacy requirements for information systems and electronic collection or maintenance of PII in the early stages of system acquisition/development. This includes completing a PIA in accordance with the requirements of Public Law 107-347, Section 208 of the E-Government Act of 2002, and DoD 5400.16-R.

(4) Ensure personnel, including contractors, who have access to PII complete appropriate Privacy training as required by 5 U.S.C. 552a, 32 CFR part 310, subpart H, and Part II of DoD Policy "Safeguarding Against and Responding to Breaches of PII" as follows:

(i) Orientation Training: Training that provides individuals with a basic understanding of the requirements of 5 U.S.C. 552a as it applies to the individual's job performance. The training is for all personnel, as appropriate, and should be a prerequisite to all other levels of training.

(ii) Specialized Training: Training that provides information as to the application of specific provisions of this part to specialized areas of job performance. Personnel of particular concern include, but are not limited to personnel specialists, finance officers, special investigators, paperwork managers, public affairs officials, information technology professionals, and any other personnel responsible for implementing or carrying out functions under this part.

(iii) Management Training: Training that provides managers and decision makers considerations that they should take into account when making management decisions regarding the Privacy program.

(iv) Privacy Act (5 U.S.C. 552a) SOR Training: All individuals who work with a Privacy Act (5 U.S.C. 552a) SOR are trained on the provisions of the 5 U.S.C. 552a SORN(s) they work with, 32 CFR Part 310, and this part.

(5) Ensure all instructions, directives, publications, policies, MOAs, MOUs, data sharing agreements, data transfer agreements, data use agreements, surveys (including web-based or electronic surveys), and forms that involve the collection, retention, use, access, sharing, or maintenance of PII are coordinated with the Chief of the OIP.

(6) Ensure that any suspected or confirmed breaches of PII, or potential breaches of PII, are immediately reported to the Chief of the OIP in accordance with NGB Memorandum 380-16/33-361 (Available at **http://www.nationalguard.mil/sitelinks/links/NGB%20Memorandum%20380-16%2033-361,%20PII%20Incident%20Response%20Handling.pdf**).

(7) Ensure policies and administrative processes within their directorates are evaluated to ensure compliance with the procedures in this part.

(h) System Managers. System Managers will:

(1) Report any changes to their existing SORN(s) to the Chief of the OIP for publishing in the FR at least 90 working days before the intended change to the system.

(2) Review their published SORN(s) on a biennial basis and submit updates to the Chief of the OIP as necessary.

(3) Ensure appropriate training is provided for all users, to include contractors, which have access to records covered by their published system notice.

(4) Ensure safeguards are in place to protect all records containing PII (electronic, paper, etc.) from unauthorized access, use, disclosure, alteration, and/or destruction using guidelines found in 32 CFR part 310, subpart B, 32 CFR part 310, Appendix 1, and DoDM 5200.01, Volume 4.

(5) Assist in responding to any complaints and inquiries regarding the collection or maintenance of, or access to information covered by their published SORN(s).

(6) Process all 5 U.S.C. 552a requests for access and amendment, as outlined in section 6 of 32 CFR part 329.

(7) Maintain a record of disclosures for any records covered by a SORN using a method that complies with 32 CFR part 310, subpart E when disclosing records outside of the agency (DoD). Such disclosures will only be made when permitted by a Routine Use published in the SORN.

(i) As required by 5 U.S.C. 552a and 32 CFR part 310, subpart E, the disclosure accounting will be maintained for 5 years after the disclosure, or for the life of the record, whichever is longer. The record may be maintained with the record disclosed, or in a separate file within the office's official record keeping system.

(ii) Pursuant to 5 U.S.C. 552a and 32 CFR part 310, subpart E, the disclosure accounting will include the release date, a description of the information released, the reason for the release; and, the name and address of the recipient.

§ 329.6 Procedures.

(a) Publication of Notice in the FR.

(1) A SORN shall be published in the FR of any record system meeting the definition of a SOR, as defined by 5 U.S.C. 552a.

(2) System Managers shall submit notices for new or revised SORNs through their Director to the Chief of the OIP for review at least 90 working days prior to implementation.

(3) The Chief of the OIP shall forward complete SORNs to the Defense Privacy and Civil Liberties Office (DPCLO), or the respective service that has the statutory authority to publish the SORN, for review and publication in the FR in accordance with 32 CFR part 310, subpart G. Following the OMB comment period, the public is given 30 days to submit written data, views, or arguments for consideration before a SOR is established or modified.

(b) Access to Systems of Records Information.

(1) As provided by 5 U.S.C. 552a, records shall be disclosed to the individual they pertain to and under whose individual name or identifier they are filed, unless exempted by the provisions in 32 CFR part 310, subpart F, and section 7 of 32 CFR part 329. If an individual is accompanied by a third party, or requests a release to a third party, the individual shall be required to furnish a signed access authorization granting the third party access conditions according to 32 CFR part 310, subpart D.

(2) Individuals seeking access to records that pertain to themselves, and that are filed by their name or other personal identifier, may submit the request in person, by mail, or by e-mail. All requests for access must be in accordance with these procedures:

(i) Any individual making a request for access to records in person shall show personal identification to the appropriate System Manager, as identified in the SORN published in the FR, to verify his or her identity, according to 32 CFR part 310, subpart D.

(ii) Any individual making a request for access to records by mail or e-mail shall address such request to the System Manager. If the System Manager is unknown, the individual may inquire to NGB-JA/OIP: AHS-Bldg 2, Suite T319B, 111 S. George Mason Drive, Arlington VA 22204-1382, or e-mail privacy@ng.army.mil for assistance in locating the System Manager.

(iii) Requests for access shall include a mailing address where the records should be sent and include either a signed notarized statement or a signed unsworn declaration to verify his or her identity to ensure that they are seeking to access records about themselves and not, inadvertently or intentionally, the records of others. The Privacy Act (5 U.S.C. 552a) provides a penalty of a misdemeanor and a fine of not more than $5,000 for any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses. If making a declaration, it shall read as follows:

(A) Inside the US: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

(B) Outside the US: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

(iv) All requests for records shall describe the record sought and provide sufficient information to enable the records to be located (e.g. identification of the SORN, approximate date the record was initiated, originating organization, and type of document).

(v) All requesters shall comply with the procedures in 32 CFR part 310, subpart D for inspecting and/or obtaining copies of requested records.

(vi) Requestors affiliated with the DoD may not use official government supplies or equipment to include mailing addresses, work phones/faxes, or DoD-issued e-mail accounts to make requests. If requests are received using DoD equipment, the requestor will be advised to make a new request, using non-DoD equipment, and processing of their request will begin only after such new request is received.

(3) The System Manager shall mail a written acknowledgement of the request for access to the individual within 10 working days of receipt. The acknowledgement shall identify the request and may, if necessary, request any additional information needed to access the record, advising the requestor that they have 20 calendar days to reply. No acknowledgement is necessary if the request can be reviewed and processed, to include notification to the individual of a grant or denial of access, within the 10 working day period. Whenever practical, the decision to grant or deny access shall be made within 30 working days. For requests presented in person, written acknowledgement may be provided at the time the request is presented.

(4) When a request for access is received, System Managers shall promptly take one of three actions on requests to access records:

(i) If no portions of the record are exempt, pursuant to the published SORN, 32 CFR part 310, subpart F, and section 7 of 32 CFR part 329, the request for access shall be granted and the individual will be provided access to all records about him or her. If there is information within the record not about the record subject (e.g. third party information) that information will be removed and referred to the Chief of the OIP for processing under 5 U.S.C. 552, pursuant to 32 CFR part 286.

(ii) If the System Manager finds that the record, or portions of the record, is exempt from access pursuant to the published SORN, 32 U.S.C. part 310, subpart F, and section 7 of 32 U.S.C. part 329, they will refer the recommended denial to the Chief of the OIP, through their Director, within 10 working days of receipt. The referral will include the following:

(A) Written recommendation for denial explaining which portion(s) of the record should be exempt from access and a discussion for why the record, or portions of the record, should be denied.

(B) The record, or portions of the record, being recommended for denial. If only portions of records are recommended for denial they must be clearly marked or highlighted.

(C) The original request and any correspondence with the requestor.

(D) A clean copy of the record.

(iii) If the request for access pertains to a record controlled and maintained by another Federal agency, but in the temporary custody of the NGB, the records are the property of the originating Component. Access to these records is controlled by the system notice and rules for the originating component/agency. Such requests shall be referred to the

originating component/agency and the requestor will be notified in writing of the referral and contact information for the component/agency.

(5) The Chief of the OIP will use the following procedures for processing any recommended denials of access:

(i) The specific reason for denial cited by the System Manager will be evaluated and a recommendation will be presented to the denial authority.

(ii) If the request for access is denied, a written letter will be sent to the requestor using procedures outlined in 32 CFR part 310, subpart D. The requestor will be advised they have 60 calendar days to appeal the decision to deny access. Appeals should be sent to: NGB Chief Counsel, 1636 Defense Pentagon, Room 1D164, Washington DC 20301-1636. The requester must provide proof of identity or a sworn declaration with their appeal, as outlined in 32 CFR part 310, subpart D.

(iii) If the request for access should be granted, the access request will be directed back to the System Manager to process.

(6) The Chief Counsel will use the following procedures for any appeals received:

(i) The Chief Counsel will notify the Chief of the OIP that an appeal has been received and will request the administrative record of the initial denial.

(ii) The Chief of the OIP will provide an exact copy of all records from the initial denial to the Chief Counsel within 10 working days.

(iii) The Chief Counsel will review the appeal and make a final determination on whether to grant or deny the appeal.

(A) If the appellate authority denies the appeal, he or she will provide a formal written notification to the requestor using the procedures outlined in 32 CFR part 310, subpart D and will provide a copy of the response to the Chief of the OIP.

(B) If the appellate authority grants the appeal, he or she will notify the Chief of the OIP and the Directorate that recommended the denial that the individual is being given access to the record. The Chief Counsel will provide a subsequent notification to the requestor advising that his or her appeal has been granted, and will provide the requestor access to his or her record.

(iv) All appeals should be processed within 30 working days after receipt by the Chief Counsel. If the Chief Counsel determines that a fair and equitable review cannot be made within that time, the individual shall be informed in writing of the reasons for the delay and of the approximate date the review is expected to be completed.

(7) There is no requirement that an individual be given access to records that are not in a group of records that meet the definition of a SOR in 5 U.S.C. 552a.

(8) No verification of identity shall be required of an individual seeking access to records that are otherwise available to the public.

(9) Individuals shall not be denied access to a record in a SOR about themselves because those records are exempted from disclosure under 32 CFR part 285. Individuals may only be denied access to a record in a SOR about themselves when those records are exempted from the access provisions of 32 CFR part 310, subpart F, and this part.

(10) Individuals shall not be denied access to their records for refusing to disclose their Social Security Number (SSN), unless disclosure of the SSN is required by statute, by

regulation adopted before January 1, 1975, or if the record's filing identifier and only means of retrieval is by the SSN (reference 5 U.S.C. 552a, note, Executive Order 9397).

(c) Access to Records or Information Compiled for Law Enforcement Purposes.

(1) All requests by individuals to access records about themselves are processed under 5 U.S.C. 552, 5 U.S.C. 552a as well as 32 CFR part 286, 32 CFR part 310, subpart D to give requesters a greater degree of access to records on themselves, regardless of which Act is cited by the requestor for processing.

(2) Records (including those in the custody of law enforcement activities) that have been incorporated into a SOR exempted from the access conditions of 5 U.S.C. 552a and 32 CFR part 310, subpart D will be processed in accordance with 5 U.S.C. 552a, 32 CFR part 310, subpart D, and this part. Individuals shall not be denied access to records solely because they are in an exempt system. They will have the same access that they would receive under 5 U.S.C. 552 and 32 CFR part 286.

(3) Records systems exempted from access conditions will be processed under 5 U.S.C. 552 and 32 CFR part 286, or 5 U.S.C. 552a and 32 CFR part 310, subpart D, depending upon which gives the greater degree of access.

(4) If a non-law enforcement element has temporary custody of a record otherwise exempted from access under 32 CFR part 310, subpart F for the purpose of adjudication or personnel actions, they shall refer any such access request, along with the records, to the originating agency and notify the requestor of the referral.

(d) Access to Illegible, Incomplete, or Partially Exempt Records.

(1) An individual shall not be denied access to his or her record or a copy of the record solely because the physical condition or the format of the record does not make it readily

available (e.g. record is in a deteriorated state or on a magnetic tape). The document will be prepared as an extract, or it will be exactly recopied.

(2) If a portion of the record contains information that is exempt from access, an extract or summary containing all of the information in the record that is releasable shall be prepared by the System Manager.

(3) When the physical condition of the record makes it necessary to prepare an extract for release, the extract shall be prepared so that the requestor will understand it.

(4) The requester shall be given access to any deletions or changes to records that are accessible.

(e) Access to Medical Records.

(1) Medical records and other protected health information (PHI) shall be disclosed to the individual pursuant to Chapter 11 of DoD 6025.18-R, DoD Health Information Privacy Regulation (Available at http://www.dtic.mil/whs/directives/corres/pdf/602518r.pdf) and 32 CFR part 310, subpart D.

(2) The individual may be charged reproduction fees for copies or records as outlined in 32 CFR part 310, subpart D.

(f) Amending and Disputing Personal Information in Systems of Records.

(1) The System Manager shall allow individuals to request amendments to the records covered by their system notice to the extent that such records are not accurate, relevant, timely, or complete. Amendments are limited to correcting factual matters and not matters of official judgment, such as performance ratings, promotion potential, and job performance appraisals.

(2) Individuals seeking amendment to records that pertain to themselves, and that are filed or retrieved by their name or other personal identifier, may submit a request for amendment in person, by mail, or by e-mail. All requests for amendment must be in accordance with the following:

(i) Any individual making a request for amendment to records in person shall show personal identification to the appropriate System Manager, as identified in the SORN published in the FR, to verify his or her identity, as outlined in 32 CFR part 310, subpart D.

(ii) Any individual making a request for amendment to records by mail or e-mail shall address such request to the System Manager. If the System Manager is unknown, they may inquire to NGB-JA/OIP: AHS-Bldg 2, Suite T319B, 111 S. George Mason Drive, Arlington VA 22204-1382, or e-mail privacy@ng.army.mil for assistance in locating the System Manager.

(iii) Requests for amendment shall include a mailing address where the decision on the request for amendment can be sent and include either a signed notarized statement or a signed unsworn declaration to verify his or her identity to ensure that they are seeking to amend records about themselves and not, inadvertently or intentionally, the records of others. The Privacy Act (5 U.S.C. 552a) provides a penalty of a misdemeanor and a fine of not more than $5,000 for any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses. The declaration shall read as follows:

(A) Inside the US: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

(B) Outside the US: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

(iv) All requests for amendment must include all information necessary to make a determination on the request for amendment, as outlined in 32 CFR part 310, subpart D.

(v) Requestors affiliated with the DoD may not use official government supplies or equipment to include mailing addresses, work phones/faxes, or DoD-issued e-mail accounts to make requests for amendment. If requests are received using DoD equipment, the requestor will be advised to make a new request, using non-DoD equipment, and processing of their request will begin only after such new request is received.

(3) When a request for amendment is received, the System Manager shall:

(i) Mail a written acknowledgement of the request for amendment to the individual within 10 working days of receipt. Such acknowledgement shall identify the request and may, if necessary, request any additional information needed to make a determination, advising the requestor that they have 20 calendar days to reply. No acknowledgement is necessary if the request can be reviewed and processed, to include notification to the individual of a grant or denial of amendment within the 10 working day period. Whenever practical, the decision to amend shall be made within 30 working days. For requests presented in person, written acknowledgement may be provided at the time the request is presented.

(ii) Determine whether the requester has adequately supported his or her claim that the record is inaccurate, irrelevant, untimely, or incomplete.

(A) If it is determined the individual's request for amendment is being granted, the System Manager will proceed to amend the records in accordance with existing statutes, regulations, or administrative procedures. The requestor will then be notified in writing of the agreement to amend and all previous holders of the records will be notified of the amendment as required by 32 CFR part 310, subpart D.

(B) If it is determined that any, or all, of the record should not be amended, the original request, along with the record requested for amendment, and justification for recommended denial action shall be forwarded through their Director to the Chief of the OIP within 10 working days of receipt for a decision by the IDA.

(C) If the request for an amendment pertains to a record controlled and maintained by another Federal agency, the amendment request shall be referred to the appropriate agency and the requestor will be notified in writing of the referral and contact information for the agency.

(4) The Chief of the OIP will use the following procedures for any recommended denials of amendment:

(i) The specific reason for denial of amendment cited by the System Manager shall be evaluated and a recommendation presented to the IDA on whether to support the recommendation to deny amendment to the record.

(ii) If the request to amend the record is denied, a written letter will be sent to the requestor using procedures outlined in 32 CFR part 310, subpart D. If an individual disagrees with the denial decision, he or she may file an appeal within 60 calendar days of receipt of the denial notification. Appeals should be sent to: NGB Chief Counsel, 1636 Defense Pentagon, Room 1D164, Washington DC 20301-1636.

(5) The Chief Counsel will use the following procedures for any appeals received:

(i) The Chief Counsel will notify Chief of the OIP that an appeal has been received and request an exact copy of the administrative record be provided within 10 working days.

(ii) The Chief Counsel will review the appeal and make a final determination on whether to grant or deny the appeal.

(A) If the Chief Counsel denies the appeal, a written letter will be provided to the requestor using the procedures outlined in 32 CFR part 310, subpart D including notification to the requestor that they may file a statement of disagreement. A brief statement will be prepared by the NGB Chief Counsel summarizing the reasons for refusing to amend the records and a copy will be provided to the Chief of the OIP and the System Manager.

(B) If the appellate authority grants the appeal, the procedures outlined in 32 CFR part 310, subpart D and this part will be followed. The System Manager will be responsible for informing all previous recipients of the amendment when a disclosure accounting has been maintained in accordance with 32 CFR part 310, subpart E.

(iii) All appeals should be processed within 30 working days after receipt by the Chief Counsel. If the Chief Counsel determines that a fair and equitable review cannot be made within that time, the individual shall be informed in writing of the reasons for the delay and of the approximate date the review is expected to be completed.

(g) Disclosure of Disputed Information. If the appellate authority determines the record should not be amended and the individual has filed a statement of disagreement, the following procedures will be used:

(1) The System Manager that has control of the record shall annotate the disputed record so it is apparent to any person to whom the record is disclosed that a statement has been filed. Where feasible, the notation itself shall be integral to the record.

(2) Where disclosure accounting has been made, the System Manager shall advise previous recipients that the record has been disputed and shall provide a copy of the individual's statement of disagreement, and the statement summarizing the reasons for the NGB refusing to amend the records in accordance with 32 CFR part 310, subpart D.

(3) The statement of disagreement shall be maintained in a manner that permits ready retrieval whenever the disputed portion of the record is disclosed.

(4) When information that is the subject of a statement of disagreement is subsequently requested for disclosure, the System Manager will follow these procedures:

(i) The System Manager shall note which information is disputed and provide a copy of the individual's statement in the disclosure.

(ii) The System Manager shall include the summary of the NGB's reasons for not making a correction when disclosing disputed information.

(5) Copies of the statement summarizing the reasons for the NGB refusing to amend the records will be treated as part of the individual's record; however, it will not be subject to the amendment procedure outlined in 5 U.S.C. 552 and 32 CFR part 310, subpart D.

(h) Penalties.

(1) Civil Action. An individual may file a civil suit against the NGB or its employees if the individual feels certain provisions of 5 U.S.C. 552a have been violated.

(2) Criminal Action.

(i) Criminal penalties may be imposed against any officer or employee for the offenses listed in subsection I of 5 U.S.C. 552a.

(ii) An officer or employee of NGB may be found guilty of a misdemeanor and fined up to $5,000 for a violation of the offenses listed in subsection I of 5 U.S.C. 552a.

(i) Litigation Status Sheet. Whenever a complaint citing 5 U.S.C. 552a is filed in a U.S. District Court against the NGB, or any employee of NGB, the Chief of Litigation and Employment Law shall:

(1) Promptly notify the Chief of the OIP of the complaint using the litigation status sheet in 32 CFR part 310, Appendix H. This status sheet will be provided to the DPCLO, or the respective service(s) involved in the litigation.

(2) Provide a revised litigation status sheet to the Chief of the OIP at each stage of the litigation for submission to the DPCLO, or the respective service(s) involved.

(3) When a court renders a formal opinion or judgment, copies of the judgment or opinion shall be provided to the Chief of the OIP who will provide them to DPCLO, or the respective service(s) involved, along with the litigation status sheet reporting the judgment or opinion.

(j) Computer Matching Programs. All requests for participation in a matching program (either as a matching agency, or a source agency) shall be submitted directly to the DPCLO for review and compliance, following procedures in 32 CFR part 310, subpart L. The Directorate shall submit a courtesy copy of such requests to the Chief of the OIP.

§ 329.7 Exemptions.

(a) General Information. There are two types of exemptions, general and specific. The general exemption authorizes the exemption of a SOR from all but a few requirements of 5 U.S.C. 552a. The specific exemption authorizes exemption of a SOR or portion

thereof, from only a few specific requirements. If a new SOR originates for which an exemption is proposed, or an additional or new exemption for an existing SOR is proposed, the exemption shall be submitted with the SORN. No exemption of a SOR shall be considered automatic for all records in the system. The System Manager shall review each requested records and apply the exemptions only when this will serve significant and legitimate purpose of the Federal Government.

(b) Exemption for Classified Material. All SOR maintained by the NGB shall be exempt under section (k)(1) of 5 U.S.C. 552a to the extent that the systems contain any information properly classified under Executive Order 13526 and that is required by that Executive Order to be kept secret in the interest of national defense or foreign policy. This exemption is applicable to parts of all systems of records including those not otherwise specifically designated for exemptions herein which contain isolated items of properly classified information.

(c) Exemption for Anticipation of a Civil Action or Proceeding. All systems of records maintained by the NGB shall be exempt under section (d)(5) of 5 U.S.C. 552a, to the extent that the record is compiled in reasonable anticipation of a civil action or proceeding.

(d) General Exemptions. No SOR within the NGB shall be considered exempt under subsection (j) or (k) of 5 U.S.C. 552a until the exemption rule for the SOR has been published as a final rule in the FR.

(e) Specific exemptions.

(1) System identifier and name: INGB 001, Freedom of Information Act (5 U.S.C.) and Privacy Act (5 U.S.C. 552a) Case Files.

(i) Exemption: During the course of a 5 U.S.C. 552 or 5 U.S.C. 552a action, exempt materials from other systems of records may, in turn, become part of the case records in this system. To the extent that copies of exempt records from those other systems of records are entered into this 5 U.S.C. 552 or 5 U.S.C. 552a case record, the NGB hereby claims the same exemptions for the records from those other systems that are entered into this system, as claimed for the original primary SOR which they are a part.

(ii) Authority: 5 U.S.C. 552a, sections (j)(2),(k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(iii) Reasons: Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this SOR. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(2) System identifier and name: INGB 005, Special Investigation Reports and Files.

(i) Exemption: Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a SOR used in personnel or administrative actions. Any portion of this SOR which falls within the provisions of 5 U.S.C. 552a(k)(2) may be exempt from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

(ii) Authority: 5 U.S.C. 552a, section (k)(2).

(iii) Reasons:

(A) From subsection (c)(3) because to grant access to the accounting for each disclosure as required by 5 U.S.C. 552a, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(B) From subsections (d) and (f) because providing access to investigative records and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and

unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under 5 U.S.C. 552a would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; enable individuals to conceal their wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(C) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(D) From subsections (e)(4)(G) and (H) because this SOR is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(E) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants.

DATED: April 15, 2013.

PATRICIA TOPPINGS

OSD Federal Register Liaison Officer

Department of Defense

[FR Doc. 2013-09619 Filed 04/23/2013 at 8:45 am; Publication Date: 04/24/2013]